PURPOSE

Computer hardware, software, email and local area network systems are intended for authorized business only. All Michigan Department of Health and Human Services (MDHHS) employees, contractors, interns and others accessing MDHHS computers and/or data by any means must comply with the State of Michigan Technical Standards found in the Administrative Guide to State Government 1300 Information Standards and Planning.

For term definitions, see Public Act 53 of 1979, Sections 752.792 and 752.793.

POLICY

There are three basic components of access control: authentication, authorization, and accountability.

- Users, including technical staff, must not attempt to gain access to computer resources by circumventing established sign on and security procedures for personal computers and networks except as necessary to perform job function.
- Users must protect the integrity of computer systems and data by maintaining the secrecy of assigned/chosen passwords.
- Do not duplicate MDHHS purchased software or copyrighted manuals for other than archival or backup purposes. Duplication for other purposes is a violation of this policy and may violate U.S. copyright law.
- The Department of Management and Budget (DTMB) approves and installs software for MDHHS users; do not bring in or download software that is not department purchased/licensed or approved.
- Do not use MDHHS computer systems for access to, display of or distribution of indecent or obscene materials, material that is illegal, racially or sexually offensive, threatening, demeaning or derogatory.
- Users must make all reasonable efforts to safeguard computer hardware from theft, and software from infection from viruses.
- Users shall not damage, alter or disrupt computer systems.

- User shall not install devices that block access to computer systems.

Any person subject to this policy who fails to comply is subject to disciplinary action up to and including dismissal.

These standards require security controls, authorized access and use of information systems. The DTMB-0161, Network User ID Request, website is used to create, modify and delete computer access accounts. Only authorized requestors can complete the process.

For a list of user access processes for MDHHS applications, see the MDHHS Employee Application Security Access and Password Reset Guide.

PROCEDURE

DTMB Research Analysis Deployment and Reporting (RADAR)

The human resources (HR) liaison sends an email to the Bureau of Organizational Services, Onboarding Support Services (OSS) at MDHHS-Onboarding@michigan.gov when an individual is hired. OSS is responsible to procure computers for all new MDHHS employees.

OSS then sends an email with instructions to the new worksite location so the information technology (IT) liaison can order equipment for the new employee according to the computer request guidelines.

To order equipment for all new employees the IT submits an electronic RADAR request form @ Inside Michigan/Service Catalog/Desktop and Laptop Service/Links and Documents.

Information Technology Resource Acquisition - Commodities System (ITRAC)

The IT liaison for former Department of Community Health (DCH) departments who have retained DCH purchasing PCA codes and indexes uses RADAR ***and*** Information Technology Resource Acquisition - Commodities System (ITRAC) to purchase computers for employee use; see APO-500, Information Technology (IT) Commodities Purchasing Request.

Onboarding completes the ITRAC for all other employees.

Note: For all ITRAC and RADAR requests please allow 4 to 6 weeks for delivery to work unit.

Employee Transfers

Authorized requestors must submit a DTMB-0919, Telecommunications Invoice Coding Change Request (Automated Electronic Form), to change the billing from the previous county's Index and PCA code to the current county's Index and PCA code to transfer equipment with a transferring employee.

Computer Protocols

To prevent unauthorized access:

- At the end of each workday, the user should power off the computer.
- Users who plan to leave their computers unattended should immediately log off network-accessible resources, lock or hibernate the device.
- Do not store State of Michigan (SOM) sensitive data on any portable device. An example of one type of sensitive data is personally identifying information (PII). This is data that can reasonably identify individuals and, if disclosed, could lead to identity theft or fraud; (for example name, address, telephone numbers, date of birth etc.).

BYOD

MDHHS does not participate in the use of privately owned devices or Bring Your Own Device (BYOD) Program; see Inside Michigan/DTMB/Bring Your Own Device program (under the websites column).

REFERENCES

Fraudulent Access to Computers, Computer Systems, and Computer Networks, MCL 752.791 et seq.

The following references posted at inside.michigan.gov/DTMB.

Note: Administrative Policies are available to SOM users only:

- DTMB Administrative Policy 900.02 Access Control

- Administrative Guide to State Government Policy 2510, Information Access.
- Work Resources/Policies, Standards & Procedures/IT Technical Policies, Standards & Procedures/1340.00.020.01, Access Control Standard.
- 13400.00.020.02, Desktop Log-off and System Shutdown Standard Information Technology.